GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:3098
ANSWERED ON:16.03.2016
Net Banking Fraud
Kaushik Shri Ramesh Chander

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether instances of scams using IP addresses from abroad have come to the notice of the Government;
(b) if so, the details thereof and the number of cases registered in this regard, State-wise;
(c) whether the Government proposes to provide training to State police and cyber crime cell to prevent such scams; and
(d) whether the Government is making any plan in collaboration with the Government of other countries to stop the misuse of IP addresses and if so, the details thereof and the time by which it is likely to be implemented?

Answer

(a): Several cyber attack techniques are used in combination while committing scams and net banking frauds. The fraudulent activities comprising of phishing, lottery scams, ATM/Credit Card frauds, internet banking frauds, and other banking frauds involve usage of e-mail to trick the users to steal their identity credentials and commit fraud. The Indian Computer Emergency Response Team (CERT-In) receives reports regarding phishing incidents affecting users of online banking. As per information reported to and tracked by CERT-In, 534 Phishing Incidents were reported in year 2015. In 342 incidents, the phishing websites are hosted in countries outside India involving Internet Protocol (IP) addresses from abroad.

(b): As per the data made available by Reserve Bank of India (RBI), 8765, 9500, 13083 and 11997 cases related to ATM/ Credit/ Debit Cards & Net Banking related frauds were reported by the banks during the year 2012-13,2013-14,2014-15 and 2015-16 (upto December 2015) respectively. Details regarding involvement of scams using IP addresses from abroad are not available with RBI. Central Bureau of Investigation (CBI) registered one case in the year 2014 involving IP address outside the country.

(c): Government has taken various steps to provide training to Law Enforcement agencies including State police to prevent cyber crimes and scams. Such steps include:

i. Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.

ii. Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.

iii. Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs, set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation.

iv. Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

v. Number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed indigenously and such tools are being used by Law Enforcement Agencies.

vi. Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

vii. Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States.

(d): The Indian Computer Emergency Response Team (CERT-In) receives reports of cyber security incidents and analyses the same. For resolution of incidents involving IP addresses outside the country, CERT-In devises response measures in coordination with its counterpart agencies in foreign countries. Besides this, Memorandum of Understanding (MoU) are signed between CERT-In and overseas CERTs for enhancing cooperation in the area of cyber security for effective resolution of cyber security incidents and mitigation of cyber attacks.

****